Method for the Secure Transmission of Messages

Field of the Invention

The present invention relates to a method and encryption system for the secure transmission of messages between at least two users of a telecommunications network.

Related Technology

Because computers have penetrated nearly every aspect of life and there is an increasing trend toward networking them in extensive telecommunications networks, the stream of data traffic between a wide variety of computers has grown enormously. Much of the information exchanged is confidential and must and/or should be protected against access by unauthorized third parties, which means there is a great need for cryptographic means of securing this data traffic. Simple cryptographic methods, however, are no match for cryptographic analysis using computers, giving rise to enormous interest in encryption methods that provide security even when computers with new kinds of decryption methods are used.

The same is also true when exchanging information over the telephone or between fax machines, since the use of the latest computer technology, combined with automatic word recognition techniques, makes it possible, in business as well as personal environments, to easily record, find at a later time, and evaluate practically any word sent over public transmission channels. In non-business applications, at least, people are practically defenseless at the moment against this type of intervention into their private lives, since they lack adequate access to the necessary encryption and decryption methods as well as apparatus required for carrying out these methods. In addition, a large portion of the known encryption methods that are usually considered to be relatively secure allow unauthorized third parties to gain access to the information exchanged by using very powerful computers and/or new types of

decryption methods. This could theoretically also result through government seizure of the keys used.

The only encryption methods that are presently considered to be absolutely secure against computer-based decryption attempts are those in which the sender and recipient of a message both use the same secret, random key, which is the same length as the message itself and is used only once for encrypting the message.

Summary of the Invention

It is therefore an object of the present invention to provide a method for individually generating secret, random keys of this type and for exchanging the generated keys between at least two users of a telecommunications network in order to encrypt information exchanged over the telephone, by fax or PC in a way that ensures its privacy. It is also an object of the present invention to provide an encryption system for carrying out this method using the corresponding technical equipment.

The present invention provides a method for the secure transmission of messages between at least two users of a telecommunications network, including the following steps:

a) a secret, random binary key of a great length is generated by a key generator (10);

b) this key is recorded on at least two portable data media (12), and these data media (12) are output by the key generator (10), with the users each receiving one data medium (12) containing the key;

c) these data media (12) are inserted into reading devices (14) which are each assigned to telecommunications equipment (16) employed by the users for message transmission, and the keys recorded on the data media (12) are read by the reading devices (14);

d) a connection is set up between the telecommunications equipment (16) employed by the users for message transmission;

e) proper insertion of the data media is checked and the read-in keys compared by logistics devices (18) which are respectively assigned to the telecommunications equipment (16) employed by the users for message transmission;

f) if the keys match, the messages to be transmitted are encrypted using at least one portion of the key.

The present invention also provides an encryption system for carrying out a method for the secure transmission of messages between at least two users of a telecommunications network, characterized by

- at least one key generator (10) having a device for generating a random, binary key of a great length, a device for recording the generated key on at least two portable data media (12), and a device for outputting the recorded data media (12);
- at least two reading devices (14) for reading the key from the recorded data media (12), with the reading devices (14) being assigned to the telecommunications equipment (16) employed by the users for message transmission;
- at least two logistics devices (18) for checking the proper insertion of the data media and for comparing the read-in keys, with the logistics devices (18) respectively being assigned to the telecommunications equipment (16) employed by the users for message transmission; and
- at least two encryption and/or decryption devices for encrypting and/or decrypting messages to be transmitted or received, using at least one portion of the read-in key if the keys match, with the encryption and/or decryption devices respectively being assigned to the telecommunications equipment (16) employed by the users for message transmission.

Brief Description of the Drawings

Special features and advantages of an encryption method according to the present invention, an encryption system according to the present invention for carrying out this method, and the corresponding technical equipment of this system are explained

in the following detailed description of an exemplary embodiment, based on the drawings, in which:

Fig. 1 shows a schematic depiction of an encryption system according to an embodiment of the present invention; and

Fig. 2 shows a flow chart of an encryption method according to the present invention.

Detailed Description

Figure 1 shows a key generator 10 for generating a random binary key of a great length (Fig. 2 block 102) which, in the present embodiment, is produced by a built-in optical random number generator with a beam splitter (not shown), like the one described in German Patent Application No. 196 41 754.6, which is hereby incorporated by reference herein. However, it is also possible to use a random number generator in which the spontaneous emission of a photon in electrically or optically excited matter or radioactive decay is used for generating the key. The use of a physical noise-generating process or another suitable physical process is also conceivable.

The generated key is then recorded, without being stored internally, on at least two portable data or key media 12 by a recording device (not shown) built into key generator 10 and output in this form to a user (Fig. 2 block 104), with the user being able to freely select the number and possibly also the type of data media output using an input keyboard (not shown). As in the present embodiment, CDs can be used as data media 12. However, the key can also be stored and output on devices such as magnetic tapes, suitable semiconductor storage devices, or another type of suitable, portable storage device.

Key generator 10 is accessible to the public in order to enable a broad segment of the population to secure their communications connections through cryptographic means. As many key generators 10 as possible should therefore be installed over a wide area,

making sure that the location where devices 10 are installed has support personnel and enjoys a certain amount of public trust, as is the case, for example, with the post office. By doing this, the danger of devices 10 being manipulated or the likelihood of the key falling into the hands of unauthorized third parties who can assign the key to a specific person is relatively low.

It is relatively easy to activate key generators 10, preferably by inserting a coin or another means of payment such as a magnetic strip card, without the user having to provide identification, or without any data on the magnetic strip card being stored. This further increases anonymity in issuing the keys, and thus the security of the encryption method.

However, it is also conceivable for large companies to encrypt, in the specified manner, all of their communications traffic with a recipient, such as a subsidiary or branch establishment, possibly in combination with dedicated lines. In this case, it would be worthwhile to use a separate key generator 10 that is installed in the company and is accessible to the employees of that company or to only a limited group of selected people, who, for security reasons, may have to first identify themselves by entering a personal secret number.

In light of enormous technological advances, it is also conceivable, however, that key generators 10 of the specified type can be produced so economically and with such compact dimensions in the future that they will be affordable even for private consumers, with large numbers of them even being found in private households.

Using an input keyboard (not shown), the number of specified data media 12 can be selected so that it corresponds to the number of users communicating with each other. If there is one sender and one recipient, therefore, two data media 12 are output, with the same random key being recorded on each one and with the sender and the recipient each receiving one of these data media 12. Data media 12 can also be

transferred, for example, in person or by sending them through the mail. The exchange of keys can also be made more secure by using a suitable key distribution system like the one known to those skilled in the art of encryption, for example, under the designation "quantum cryptography".

To encrypt a message, the users insert data media 12 into reading devices 14 which are assigned to telecommunications equipment 16, such as telephones, fax machines, or PCs, employed by the users (i.e., the sender of a message and the corresponding recipient of the message) for message transmission and which are used to read the implemented key from the data media (Fig. 2 block 106).

Logistics devices 18, which are also assigned to the telecommunications equipment 16 used for message transmission and which contact each other automatically when a connection is set up (Fig. 2 block 108), are used to check whether the key has been entered properly and whether the keys entered by the users correspond to each other (Fig. 2 block 110). If the keys match, encryption may take place (Fig. 2 block 112).

When a message is encrypted or decrypted, logistics devices 18 also synchronize the sender and recipient keys, or portions of these keys, and ensure that only the as yet unused portions of the random key on key media 12 are used for encryption. This is done, for example, by deleting the used portions of a key, rendering them unusable, or storing the location on the data medium that marks the end of the used portion of the key.

A binary message to be transmitted is easily encrypted, for example, by adding the key in the form of a binary code to the message (modulo 2) and subsequently transmitting the resulting random number sequence from an assigned transmission device 20 to the corresponding recipient via a transmission line 22. The random key is then subtracted from incoming encrypted messages, thus decrypting the message. The message can then be supplied to the telephone, fax machine, or other device of

the recipient. After an entire key has been used up, a new key, which does not match any other key and can also be used only once, can be obtained from any key generator 10.

Reading device 14 and logistics device 18 can be designed in a very compact and light-weight format so that they can be used separately as well as integrated into a combined device, even in portable handsets, which greatly expands the range of applications for a method according to the present invention.

In two-way calls over the telephone, encryption and transmission as well as decryption must take place during the call and during pauses in the conversation, which means that buffers may have to be provided in order to collect portions of the message prior to transmission. However, these individual components are already necessary for normal transmission and encryption as well as for reading and recording messages.

If a sender of messages would like to correspond privately with multiple recipients, he can use a separate key for each of these connections, with this key being again recorded on two identical data media 12 and the sender and recipient each receiving one data medium 12. To maintain order in this case, various data media 12 containing the keys can be inserted into an apparatus which assigns the individual keys to the selected recipients. It includes a holding device for various key media 12 and, when a connection is set up, automatically selects the correct one containing the same key as the one assigned to the selected recipient. If the key media are CDs, the apparatus resembles the CD changer of a CD player. The individual keys can be assigned either manually by the user or by a logistics device in the apparatus itself, which, prior to setting up a connection, contacts the corresponding logistics device of a recipient, checks the inserted key medium or key, and automatically selects the correct key medium or key. Once again, the keys are read from key media 12 using an integrated reading device.

It is also conceivable for both the recipient and the sender to have an apparatus in which multiple data media 12 containing keys are inserted so that the media can be processed either consecutively in a permanently specified order or in a random order determined by the sender's logistics device, which then contacts the corresponding logistics device of the recipient in order for a data medium containing the same key to be inserted at the receiving end.

Because the random keys in the method according to the present invention are recorded only on key media 12, are not known to transmission and reading devices 20 and 14, and are also used only once for encrypting a message, it is practically impossible for unauthorized third parties to break the code even when using very powerful computers and the latest encryption methods, as long as key media 12 containing the keys do not fall into the hands of unauthorized persons, which is relatively easy to prevent by taking suitable precautionary measures.